

ANALYSES

- **DIFFAMATION PAR COURRIER ÉLECTRONIQUE : UNE PREUVE PAS SI LIBRE**
- **BLOPAGE DE .FR : ENCORE UN CAS**
- **LE CONTRÔLE DES MESSAGERIES ÉLECTRONIQUES PROFESSIONNELLES**
- **L'ACHAT EN LIGNE : QUELLE SÉCURITÉ POUR LE CYBERCONSOMMATEUR**
- **BLOG ET LICENCIEMENT ABUSIF**
- **PREMIER CAS DE SUCKS EN .EU**
- **MESURES TECHNIQUES DE PROTECTION : UN DÉCRET ET UNE DÉCISION LE MÊME JOUR**

AU JOURNAL OFFICIEL

- **Décret n° 2007-663 du 2 mai 2007**
- **Décret n° 2007-602 du 25 avril 2007**
- **Arrêté du 25 avril 2007**

DÉLIBÉRATION CNIL

- **Dél. n°2007-091 du 25 avril 2007 refusant la mise en oeuvre par l'Autorité de contrôle des assurances et des mutuelles (ACAM) d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au réseau informatique (postes de travail fixes et portables). ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle**

RDTIC

REVUE DE DROIT DES TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION

La revue de droit des techniques de l'information et de la communication (RDTIC) est un service proposé par DROIT-TIC - www.DROIT-TIC.com.

Elle vous propose une synthèse non exhaustive des informations juridiques mise en ligne sur le site DROIT-TIC durant le mois écoulé. Vous y trouverez non seulement des articles (actualités, analyses, synthèses, doctrines...), mais encore des décisions de justice, la doctrine de certaines autorités administratives indépendantes et des textes normatifs.

Conseil scientifique

- Julien Le Clainche, chercheur
- François-Xavier Boulin, avocat BCTG Associés
- Anthony Grevin, juriste M6 Web
- Vincent Duseauguey, juriste M6 Web
- Julien Linsolas, juriste SFR
- Olivier Gnos, architecte logiciel
- Marie-Alix Boussard, allocataire de recherche

Informations légales

La RDTIC est protégée par les normes nationales et internationales en vigueur, notamment celles relatives à la propriété intellectuelle.

Citation : RDTIC n° XX, mois année, DROIT-TIC, p. XX.

Les articles sont la propriété de leurs auteurs. Si vous souhaitez les contacter, rendez-vous sur le site DROIT-TIC.com, rubrique "DROIT-TIC et vous", 'L'équipe de DROIT-TIC".

La lecture de la RDTIC emporte le respect des conditions d'utilisation du site DROIT-TIC qui sont disponibles à l'adresse : <http://www.droit-tic.com/index2.php?page=conditions.php>

Vous pouvez présenter vos observations, remarques, soutiens, encouragements et autres critiques constructives en écrivant à julien@droit-ntic.com.

DROIT-TIC / Julien Le Clainche, 5 rue des chênes verts, 34110 MIREVAL.

ANALYSES

■ **DIFFAMATION PAR COURRIER ÉLECTRONIQUE : UNE PREUVE PAS SI LIBRE**

Par Me. Nicole Bondoïs, Avocate et M. Raphaël Rault Juriste TIC -
BRM Avocats

■ **BLOCAGE DE .FR : ENCORE UN CAS**

Par M. Jean-François Poussard, Rédacteur en Chef MailClub.info

■ **LE CONTRÔLE DES MESSAGERIES ÉLECTRONIQUES PROFESSIONNELLES**

Par M. Nicolas Samarcq

■ **L'ACHAT EN LIGNE : QUELLE SÉCURITÉ POUR LE CYBERCONSOMMATEUR ?**

Par M. Sulliman Omarjee, Juriste

■ **BLOG ET LICENCIEMENT ABUSIF**

Par Me. Martine Ricouart-Maillet, Avocate associée, cabinet BRM.
et M. Raphaël Rault Juriste TIC - BRM Avocats

■ **PREMIER CAS DE SUCKS EN .EU**

Par M. Benjamin Vitasse, Juriste - Consultant noms de domaine

■ **MESURES TECHNIQUES DE PROTECTION : UN DÉCRET ET UNE DÉCISION LE MÊME JOUR**

Par Me. Martine Ricouart-Maillet, Avocate associée, cabinet BRM.
et M. Raphaël Rault Juriste TIC - BRM Avocats

AU J.O DES MOIS DE MAI/JUIN 2007

■ Décret n° 2007-663 du 2 mai 2007 Pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie, J.O n° 104 du 4 mai 2007 p. 7865.

■ Décret n° 2007-602 du 25 avril 2007 relatif aux conditions et aux modalités de vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise et modifiant le code du travail (deuxième partie : Décrets en Conseil d'État), J.O n° 99 du 27 avril 2007 p. 7492.

■ Arrêté du 25 avril 2007 pris en application du décret n° 2007-602 du 25 avril 2007 relatif aux conditions et aux modalités de vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise et modifiant le code du travail (deuxième partie : Décrets en Conseil d'État), J.O n° 99 du 27 avril 2007 p. 7494.

DÉLIBÉRATIONS CNIL

■ Dél. n°2007-091 du 25 avril 2007 refusant la mise en oeuvre par l'Autorité de contrôle des assurances et des mutuelles (ACAM) d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au réseau informatique (postes de travail fixes et portables). ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle

DROIT DE LA PREUVE, SIGNATURE ÉLECTRONIQUE, DROIT SOCIAL, DROIT DU TRAVAIL

DIFFAMATION PAR COURRIER ÉLECTRONIQUE : UNE PREUVE PAS SI LIBRE...

Par Me. Nicole Bondoïs,
Avocate et M. Raphaël Rault
Juriste TIC - BRM Avocats.

Suite au licenciement pour faute grave d'un chef de ventes, ce dernier a intenté une action en justice contre son employeur, considérant cette mesure comme abusive. Cette affaire a été portée devant la Chambre sociale de la Cour de cassation, qui a rendu un arrêt le 21 décembre 2006.

En l'espèce, un mail dénonçant « les augmentations de salaires hors mérite et bonne gueule » avait été rédigé par le salarié en question et avait été envoyé, selon lui, au secrétaire du comité d'entreprise, mais encore à tous les salariés de l'entreprise selon l'employeur.

La preuve du caractère public de la diffusion de mail devait être rapportée par l'employeur. Puisque ce n'est que dans cette hypothèse que constitue un délit la diffamation, définie par l'article 29 de la loi du 29 juillet 1881 sur la liberté de la presse comme « Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé ». D'où l'intérêt de déterminer précisément les destinataires du mail litigieux. A cet égard, la diffusion au seul comité d'entreprise, constituant un groupe de personnes partageant une même communauté d'intérêts, est considérée comme privée.

Par ailleurs, la Chambre criminelle de la Cour de cassation a estimé, dans un arrêt du 15 décembre 1949, que le personnel d'une entreprise ne constitue pas un public au sens de l'article 23 de la loi de 1881 précitée.

Il aurait donc fallu pour l'entreprise démontrer que le mail litigieux avait été diffusé à l'extérieur de l'entreprise. Dans un arrêt du 2 juin 2004, la Chambre sociale a ainsi jugé qu'un mail antisémite envoyé par un salarié à un tiers extérieur à l'entreprise sous une adresse électronique permettant d'identifier l'employeur était constitutif d'une faute grave.

Dans notre espèce, la Cour d'appel de Toulouse n'a pas eu à déterminer s'il y avait ou non diffusion au public. En effet, dans sa décision du 24 février 2005, elle a écarté le caractère diffamatoire du mail et a considéré le licenciement comme dépourvu de cause réelle et sérieuse en ce que l'employeur n'établissait pas la diffusion du mail aux salariés dès lors :

- qu'il ne produisait pas l'édition certifiée à partir du serveur centralisé de la messagerie intranet de l'entreprise ;
- qu'il s'était abstenu d'assurer la sauvegarde de toutes les boîtes mails en émission ou en réception.

La Cour de cassation a rejeté le pourvoi, considérant que la Cour d'appel avait souverainement apprécié comme insuffisants les éléments fournis et pouvait décider que le mail en cause « n'excédait pas les limites de la liberté d'expression du salarié ». De sorte qu'aucun motif réel et sérieux ne pouvait justifier le licenciement.

Il faut donc retenir de cet arrêt que la preuve de la diffusion publique d'un mail pèse sur le demandeur et que les éléments de preuve à rapporter sont extrêmement stricts !

ADRESSAGE, NOMS DE DOMAINE ET LIENS HYPERTEXTES, PROPRIÉTÉS INDUSTRIELLES ET COMMERCIALES

BLOPAGE DE .FR : ENCORE UN CAS

Par M. Jean-François Poussard,
Rédacteur en Chef
MailClub.info

Depuis juillet 2005, l'Afnic bloque toujours le portefeuille de noms de domaine de la société KLTE Limited..

Depuis juillet 2005, l'Afnic bloque toujours le portefeuille de noms de domaine de la société KLTE Limited. 1 144 .fr sont encore immobilisés et Klte Limited n'est pas coopérant. Une des seules manières de récupérer des noms litigieux est d'engager une procédure auprès du Centre d'arbitrage et de médiation de l'OMPI. Dernier cas en date, gerbe.fr.

Le Requéant est la société RHOVYL et a depuis plus d'un quart de siècle fait enregistrer la marque GERBE qui fait l'objet d'une protection non seulement sur le territoire français, mais également dans un certain nombre de pays étrangers. L'Expert considère que "l'enregistrement du nom de domaine litigieux par le Défendeur constitue une atteinte aux droits de tiers et en particulier, aux droits de marque du Requéant".

Déjà Les Echos, Total, Orange...

La marque GERBE étant une marque notoire, le Défendeur en utilisant à son profit le nom de domaine litigieux sans justifier de quelconques droits sur le terme GERBE, prive le Requéant de son droit légitime à exploiter le nom de domaine correspondant à sa marque dans la zone ".fr". En effet, cette rétention injustifiée prive le Requéant de clients potentiels désireux d'acquérir ses produits. L'Expert relève par ailleurs que, "*comme invoqué par le Requéant, le Défendeur a eu à connaître par le passé de nombreux litiges l'opposant à de grandes marques françaises suite à son enregistrement massif de noms de domaine (plus de 1200 ".fr") à l'été 2005, et que nombre de ces grandes marques ont obtenu gain de cause (Les Echos contre KLTE Ltd, Litige OMPI n° DFR2005-0012 ; Total SA contre KLTE Ltd ,Litige OMPI n° DFR2005-0017 ; France Telecom contre KLTE Ltd ; Litige OMPI n° DFR2005-0019 ; Orange France contre KLTE Ltd, Litige OMPI n° DFR2005-0020). Ces éléments de fait permettent de douter de la volonté réelle et sérieuse du Défendeur d'utiliser de bonne foi le nom de domaine litigieux, d'autant que depuis son enregistrement, il semble que ce nom de domaine servait à renvoyer vers une page de parking contenant des liens hypertexte pour du commerce en ligne, de surcroît en langue allemande*".

L'Expert considère ainsi "*que l'utilisation du nom de domaine par le Défendeur constitue une atteinte au principe de loyauté en matière commerciale*". L'expert ordonne la transmission au profit du Requéant du nom de domaine gerbe.fr.

C'est le quinzième nom de domaine qui est récupéré ainsi par les différents ayants droit auprès de Klte Limited, via l'OMPI.

L'Afnic a procédé à trois grands blocages ces dernières années. Le premier concernait Eurodns et a mis trente

mois à se résoudre ([lire notre article à ce sujet](#)), le second concerne Klte et est toujours en cours. Le dernier aura été express pour Guillaume.net, moins de cinq mois !



INFORMATIQUE ET LIBERTÉS, DROIT SOCIAL, DROIT DU TRAVAIL

LE CONTRÔLE DES MESSAGERIES ÉLECTRONIQUES PROFESSIONNELLES

Par M. Nicolas Samarcq,
Juriste TIC.

L'employeur peut obtenir une ordonnance l'autorisant à conserver ou établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige.

Le 23 mai dernier, la Cour de cassation¹ a apporté une nouvelle précision tendant à concilier deux droits légitimes et opposés : le respect de la sphère privée du salarié et le pouvoir de contrôle de l'employeur.

La Cour a en effet rendu son premier arrêt relatif à l'application de l'article 145 du nouveau code de procédure civile (NCPC) aux échanges de courrier électronique.

Sur le fondement de cet article, l'employeur peut obtenir, sur requête auprès du président d'un tribunal de grande instance (TGI), une ordonnance l'autorisant à conserver ou établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige².

La question posée à la chambre sociale de la Cour de cassation était de savoir si cette procédure permettait de donner mission à un huissier de justice d'accéder aux

données contenues dans l'ordinateur mis à la disposition d'un salarié par son employeur.

Plus précisément, l'ordonnance du président du TGI avait autorisé un huissier de justice à prendre connaissance et à enregistrer le contenu des messages électroniques échangés par un salarié avec deux personnes identifiées et étrangères à l'entreprise, car celle-ci le soupçonnait d'entretenir des relations constitutives de manoeuvres déloyales (à savoir la création d'une société concurrente).

En appel, les juges ont rétracté l'ordonnance et annulé le procès-verbal dressé par l'huissier, en retenant que cette procédure a eu « *pour effet de donner à l'employeur connaissance de messages personnels émis et reçus par le salarié et en déduit qu'elle porte atteinte à une liberté fondamentale³ et n'est pas légalement admissible* ».

Au contraire, la Cour de cassation a considéré, à la lumière de sa jurisprudence « Nikon »⁴, que « *le respect de la vie personnelle du salarié ne constitue pas en lui-même un obstacle à l'application des dispositions de l'article 145 du nouveau code de procédure civile dès lors que le juge constate que les mesures qu'il ordonne procèdent d'un motif légitime et sont nécessaires à la protection des droits de la partie qui les a sollicitées* ». En l'espèce, il s'agissait de protéger l'entreprise contre d'éventuels actes de concurrence déloyale commis via la messagerie électronique d'un salarié.

Le principe posé par la jurisprudence « Nikon », interdisant toute investigation unilatérale de l'employeur en vue de prendre connaissance de messages électroniques personnels de ses salariés, doit effectivement se concilier avec les moyens procéduraux légitimes offerts à l'entreprise par l'article 145 NCPC qui garantissent aux employés l'intervention et le contrôle du juge.

Enfin, il est également à remarquer que la Cour de cassation a été sensible au fait que le constat d'huissier ait été réalisé en présence du salarié, ce qui peut être dans certain cas un élément déterminant quant à la licéité de la procédure et donc de la preuve.

Dans une affaire précédente, la Cour de cassation a jugé en ce sens que « *sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé* »⁵.

En conséquence, dès lors que le contrôle s'opère sur des fichiers ou messages dits « personnels », hors la présence du salarié ou sans l'informer, la valeur probante de la preuve dépendra aussi de l'interprétation de la notion de « *risque ou événement particulier* », qui est nécessairement stricte au regard du risque d'atteinte à une liberté fondamentale protégée, notamment, par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

La Cour de cassation a ainsi jugé, dans l'arrêt précité⁶, que la découverte de photos érotiques dans un tiroir du bureau d'un salarié ne constituait pas un motif suffisant pour justifier l'accès à ses fichiers informatiques identifiés comme personnels sans l'avertir ou le faire en sa présence.

En réalité, cet arrêt applique à l'informatique une jurisprudence antérieure relative aux conditions de contrôle du contenu des armoires personnelles affectées aux salariés⁷. Selon la Cour, « *l'employeur ne peut procéder à l'ouverture de l'armoire individuelle d'un salarié que dans les cas et aux conditions prévues par le règlement intérieur et en présence de l'intéressé ou celui-ci prévenu* ». Par exception, ce contrôle est possible sans inscription au règlement intérieur et sans information préalable s'il existe un « *risque ou*

événement particulier ». Dans cette affaire, il a été jugé que la fouille ayant permis la découverte de boissons alcoolisées (3 canettes de bière), hors la présence du salarié, n'était justifiée « *par aucun risque ou événement particulier* ».

Inversement, « *les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence* »⁸.

En conclusion, il est fortement conseillé lors d'un contrôle de fichiers ou de messages électroniques d'un salarié, outre le respect de la procédure de l'article 145 NCPC, d'avertir ce dernier ou de le faire en sa présence. A défaut, en cas de contenus identifiés comme personnels, l'huissier en charge du contrôle devra s'abstenir de les ouvrir « *sauf risque ou événement particulier* ». Or, cette notion, laissée au pouvoir d'appréciation des juges, présente un certain risque juridique. En effet, s'il est envisageable de considérer que l'existence d'un risque majeur relatif à la sécurité du système informatique de l'entreprise recouvre les exigences jurisprudentielles ; en revanche, l'arrêt du 23 mai 2007 n'apporte aucun élément probant concernant des agissements déloyaux pouvant se traduire par la transmission à des tiers de données stratégiques.

Nicolas Samarcq

Juriste TIC

www.lexagone.com

:

PROPRIETES INTELLECTUELLES, DROIT DE LA CONSOMMATION, PROTECTION DU CONSUMMATEUR

MESURES TECHNIQUES DE PROTECTION : UN DÉCRET ET UNE DÉCISION LE MÊME JOUR

Par Me. Martine Ricouart-
Maillet avocate associée,
cabinet BRM. et M. Raphaël
Rault juriste TIC - BRM
Avocats.

Les dispositions du décret semblent particulièrement restrictives quant aux conditions que doivent remplir les seules personnes autorisées à saisir l'ARMT.

Instaurées par la loi sur les droits d'auteur et les droits voisins dans la société de l'information (DADVSI) du 1er août 2006, les mesures techniques de protection ont fait l'objet, le 4 avril 2007 :

- d'un décret relatif à l'Autorité de régulation des mesures techniques instituée par l'article L. 331-17 du code de la propriété intellectuelle ;
- d'une décision de renvoi de la Cour d'appel de Paris dans l'affaire « Mulholland Drive ».

1. Décret du 4 avril 2007 relatif à l'Autorité de régulation des mesures techniques instituée par

l'article L. 331-17 du code de la propriété intellectuelle

Ce décret, pris en application de la loi DADVSI, crée une section 2 intitulée « mesures techniques de protection et d'information » dans le chapitre 1er du titre III du livre III relatif au droit d'auteur du code de la propriété intellectuelle (partie réglementaire).

Cette nouvelle section contient les dispositions relatives à l'autorité de régulation des mesures techniques (ARMT) instituée par la loi DADVSI.

Prenant en compte l'importance de la coexistence pacifique entre l'exception de copie privée et la protection du droit d'auteur, le nouvel article R. 331-2 du Code de la propriété intellectuelle dispose que « Les décisions prises par l'Autorité (...) ne peuvent porter atteinte à l'exploitation normale d'une oeuvre ou d'un objet protégé par un droit de propriété intellectuelle, ni causer un préjudice injustifié aux intérêts légitimes des titulaires de droits de propriété intellectuelle ».

Le décret envisage tout d'abord **l'organisation et le fonctionnement de l'ARMT** et affirme que ses membres et rapporteurs sont tenus au secret professionnel et ne peuvent traiter une question dans laquelle ils ont un intérêt direct ou indirect.

Concernant la **procédure**, la saisine de l'ARMT se fait par LRAR ou par « transmission par voie électronique ». Le demandeur peut être un rapporteur de l'ARMT ou une association de consommateurs agréée.

Par ailleurs, le demandeur doit préciser « la nature et le contenu du projet dont la réalisation nécessite l'accès aux informations essentielles à l'interopérabilité qu'il sollicite, et justifier qu'il a demandé et s'est vu refuser cet accès ».

Lorsqu'une partie se prévaut d'un secret protégé par la loi, un système de classement en « annexe confidentielle » peut être mis en place durant la procédure.

L'interopérabilité des mesures techniques fait l'objet d'une procédure spécifique : un accord peut être trouvé entre les parties et faire l'objet d'un procès verbal du rapporteur de l'ARMT qui fixe un délai pour l'exécution de l'accord.

A défaut d'accord des parties et de l'ARMT, un rapport est établi par le rapporteur et notifié aux parties, qui disposent d'un délai de quinze jours pour prendre connaissance du dossier et effectuer leurs observations écrites.

Au terme de la procédure, l'ARMT peut, par une décision motivée, soit rejeter la demande dont elle a été saisie, soit enjoindre au titulaire des droits sur la mesure technique de prendre les mesures propres à assurer l'accès du demandeur aux informations essentielles à l'interopérabilité. Ces décisions peuvent être assorties d'injonctions et d'astreintes.

Une procédure de conciliation est également prévue pour les litiges relatifs aux exceptions au droit d'auteur et aux droits voisins.

Concernant les voies de recours, les décisions de l'ARMT sont notifiées par LRAR aux parties, qui peuvent, dans le délai d'un mois, introduire un recours en annulation ou en réformation devant la cour d'appel de Paris selon une procédure spécifique également.

2. Arrêt de renvoi de la Cour d'appel de Paris du 4 avril 2007 dans l'affaire « Mulholland Drive »

Après avoir fait l'acquisition du DVD « Mulholland Drive

», un cinéphile avait souhaité en réaliser une copie sur cassette vidéo afin de visionner le film sur un magnétoscope. Mais en raison de la présence de mesures techniques de protection insérées dans le support DVD et dont il n'était fait nullement mention sur la jaquette, la copie n'avait pu être réalisée.

Considérant qu'une atteinte avait été portée au droit de copie privée reconnu à l'utilisateur par les articles L. 122-5 et L. 211-3 du Code de la propriété intellectuelle, l'acquéreur et l'Union fédérale des consommateurs UFC Que choisir avaient alors assigné le producteur, éditeur et diffuseur du DVD « Mulholland Drive » en réparation du préjudice subi.

Dans un arrêt de la Première chambre civile de la Cour de cassation du 28 février 2006 (voir notre actualité du 31 mars 2006), les magistrats retiennent que « *l'atteinte à l'exploitation normale de l'œuvre, propre à faire écarter l'exception de copie privée, s'apprécie au regard des risques inhérents au nouvel environnement numérique quant à la sauvegarde des droits d'auteur et de l'importance économique que l'exploitation de l'œuvre, sous forme de DVD, représente pour l'amortissement des coûts de production cinématographique* » (test des trois étapes).

Il est déduit de ce « test des trois étapes » que l'exception de copie privée n'interdit en rien l'insertion dans les supports sur lesquels est reproduite une œuvre protégée, de mesures techniques de protection visant à en limiter la copie.

Allant dans le même sens, la Cour d'appel de Paris, dans son arrêt du 4 avril 2007, affirme que l'interopérabilité demandée dépasse la limite de la copie privée telle que fixée par l'article L. 122-5, 2° du Code de la propriété intellectuelle.

En effet, « *il résulte de la nature juridique de la copie*

privée que celle-ci (...) ne constitue pas un droit mais une exception légale au principe de prohibition de toute reproduction intégrale ou partielle d'une oeuvre protégée faite sans le consentement du titulaire des droits d'auteur
».

Ainsi, « il se déduit de cette qualification que si la copie privée peut être, à supposer les conditions légales remplies, opposée pour se défendre à une action, notamment en contrefaçon, elle ne saurait être invoquée comme étant constitutive d'un droit, au soutien d'une action formée à titre principal, peu important au regard du principe pas de droit pas d'action, l'existence d'une rémunération pour copie privée acquittée par les consommateurs ».

Le décret précité et la décision ci-dessus analysée démontrent que les mesures techniques de protection sont de plus en plus encadrées et protégées par les dispositions légales et la jurisprudence et semblent constituer à ce jour, malgré les critiques auxquelles elles font face, notamment chez les défenseurs de l'interopérabilité, la seule alternative à la violation des droits d'auteur envisagée pour les supports numériques.

A cet égard, les dispositions du décret semblent particulièrement restrictives quant aux conditions que doivent remplir les seules personnes autorisées à saisir l'ARMT, de sorte que l'on peut se poser la question de savoir quelle sera la réelle activité régulatrice et l'efficacité de cette nouvelle entité..

ECONOMIE NUMÉRIQUE, DROIT DE LA CONSOMMATION, PROTECTION DU CONSOMMATEUR

L'ACHAT EN LIGNE : QUELLE SÉCURITÉ POUR LE CYBERCONSOMMATEUR ?

Par M. Sulliman Omarjee,
Juriste

En clarifiant les conditions de l'achat en ligne et en renforçant les droits du cyberconsommateur, la LCEN offre une sécurité juridique déterminante au profit de l'acheteur en ligne.

Avec 17,9 millions d'acheteurs au premier trimestre 2007 contre seulement 8,2 millions en 2003, le commerce électronique affiche en France une nette progression : 63 % des internautes français ont aujourd'hui franchis le pas de l'achat en ligne contre 38% en 2003 (source : Médiamétrie, mars 2007, disponible sur le journaldunet.com).

Plusieurs raisons peuvent expliquer ce succès : tarifs attractifs, meilleure structuration des offres, meilleure ergonomie des sites en ligne...

Parmi celles-ci, l'adoption de la loi sur la Confiance dans l'Economie Numérique (LCEN) du 21 juin 2004 mérite d'être soulignée : en clarifiant les conditions de l'achat en ligne et en renforçant les droits du cyberconsommateur, la LCEN offre une sécurité juridique déterminante au profit de l'acheteur en ligne.

1 – La sécurité lors de la formation du contrat

La LCEN impose une certaine transparence de la part du Cybervendeur à l'égard du Cyberacheteur. Tout d'abord, le Cybervendeur a l'obligation d'indiquer sur son site **par un accès facile, direct et permanent** des informations précises quant à son identité (article 19 de la LCEN : nom prénom ou raison sociale ; adresse ; numéro RCS...). Le Cybermarchand doit également mettre à disposition les conditions contractuelles applicables **d'une manière qui permette leur conservation et leur reproduction** (article 1369-1 nouveau du code civil). Toute information relative au prix, même en l'absence de contrat, doit être **claire et non ambiguë** et notamment doit préciser si les taxes et les frais de livraison sont inclus.

Tant que l'offre restera accessible en ligne, le Cybermarchand en restera engagé (article 1369-1 du code civil).

L'offre doit par ailleurs énoncer toutes les étapes nécessaires à la conclusion du contrat en ligne. Ces étapes ont été définies par la LCEN et intégrées dans le code civil à l'article 1369-2 : pour que le contrat soit valablement conclu, le cyberacheteur doit avoir eu la possibilité dans un premier temps de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs ; le cyberacheteur devra dans un deuxième temps confirmer sa commande pour exprimer son acceptation et valider par conséquent la transaction.

Le Cybercommerçant a l'obligation d'accuser réception sans délai injustifié et par voie électronique de la commande qui lui a été adressée.

Echappent à ces obligations les contrats de fourniture de biens et de services conclus exclusivement par échange de courriers électronique ainsi que les contrats conclus en ligne entre professionnels.

Enfin, depuis le décret d'application du 18 février 2005, les e-commerçants ont l'obligation de conserver pendant

dix ans une trace de tout contrat de vente à distance d'un montant supérieur à 120 Euros.

2 – La sécurité quant à l'exécution de la prestation

L'article 15 de la LCEN (intégré dans le code de la consommation) instaure **une responsabilité de plein droit du Cybercommerçant à l'égard du Cyberconsommateur** : l'e-commerçant est présumé responsable de plein droit de l'inexécution ou de la mauvaise exécution de la prestation, quand bien même celle-ci serait due à un intermédiaire de la chaîne de contrat et à charge pour lui de se retourner contre cet intermédiaire. Tout Cyberacheteur s'estimant lésé pourra ainsi engager la responsabilité du Cybervendeur, même si la cause de l'inexécution ou de la mauvaise exécution de la prestation est imputable au livreur par exemple : l'avantage est considérable puisqu'il évite au consommateur d'avoir à se retourner contre une pléiade d'intermédiaires en vue d'obtenir réparation, ce qui pourrait se révéler décourageant. Au contraire, le choix de la loi est celui de la simplicité : un seul interlocuteur, donc un seul responsable.

Toutefois, le Cybercommerçant pourra s'exonérer de sa responsabilité dans trois hypothèses dont il devra apporter la preuve :

- le fait de l'acheteur
- le fait imprévisible et insurmontable d'un tiers étranger à la fourniture des prestations au contrat
- la force majeure

En pratique, ces preuves seront très difficiles à rapporter pour un Cybercommerçant comme en témoignent les quelques décisions intervenues en la matière depuis trois ans et retenant dans l'ensemble l'application du principe de la responsabilité de plein droit. Seule une décision du 7 novembre 2006 rendue par la juridiction de proximité de Courbevoie a retenue l'exonération de la responsabilité d'un Cybermarchand s'agissant de contrat

de fourniture d'accès Internet, le FAI rapportant la preuve d'une faute de l'opérateur historique France Télécom qui présentait les caractères d'un cas de force majeure.

3 – La sécurité lors du paiement de la transaction

En libéralisant la cryptologie, la LCEN autorise l'emploi par des prestataires privés de moyens techniques permettant de sécuriser l'échange de données et traditionnellement réservés aux transmissions militaires : ces moyens ont principalement pour objet **de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité** (article 30 de la LCEN). Cette libéralisation était nécessaire pour pouvoir assurer le développement du commerce électronique, l'échange de données étant au cœur du processus : ainsi le recours à ces moyens permettra de garantir l'intégrité et l'authenticité de la commande ainsi que le paiement en ligne qui en résultera. Les prestataires de cryptologies sont astreints au secret professionnel ainsi qu'à une obligation de confidentialité quant aux données qu'ils transmettent. Ils sont par ailleurs présumés responsables du préjudice causé aux personnes leur confiant des données à transmettre, en cas d'atteintes à l'intégrité ou à la confidentialité de ces données dans le cadre du processus d'envoi sécurisé. De même les tiers certificateurs sont présumés responsables du préjudice causé aux personnes qui se sont fiés aux certificats qu'ils délivrent, lorsqu'il s'avère que ces certificats ne sont pas fiables

De plus, les dispositions de l'article L 132-4 du Code Monétaire et Financier pourront s'appliquer **en cas d'utilisation frauduleuse d'une carte bancaire pour réaliser un paiement en ligne**. Selon cet article, la responsabilité du titulaire d'une carte bancaire n'est pas engagée si le paiement contestée a été effectuée frauduleusement à distance sans utilisation physique de la carte. De même, sa responsabilité n'est pas engagée en cas de contrefaçon de sa carte et si, au moment de l'opération contestée, il était en possession physique de

sa carte. Dans ce cas, le titulaire de la carte doit, dès qu'il prend connaissance de la fraude et avant l'expiration d'un délai de 70 jours, contester par écrit avoir effectué un paiement ou un retrait. L'établissement bancaire est alors dans l'obligation de lui recrediter ou de lui restituer sans frais les sommes contestées dans un délai d'un mois à compter de la réception de la contestation. La jurisprudence a pu confirmer l'obligation pour la banque de procéder au remboursement d'un débit litigieux via Internet (Cass. Com 12 décembre 2006, affaire Caisse d'Epargne), la charge du débit litigieux étant supporté par le Cybercommerçant (CA PAU, 8 février 2007, affaire Société Générale)

Par **M. Sulliman Omarjee**, Juriste

Par Sulliman OMARJEE

Juriste de Propriété Intellectuelle & NTIC à la REGION REUNION

DEA de Droit des Créations Immatérielles – LLB – WIPO (DL 101)

s.omarjee@laposte.net

INFORMATIQUE ET LIBERTÉS, DROIT SOCIAL, DROIT DU TRAVAIL

BLOG ET LICENCIEMENT ABUSIF

Par Me. Martine Ricouart-Maillet, Avocate associée, cabinet BRM. et M. Raphaël Rault Juriste TIC - BRM Avocat.

Licenciée en avril 2006 pour avoir tenu sur son blog des propos qui ont été jugés dénigrants et portant atteinte à la réputation de l'entreprise pour laquelle elle travaillait, une jeune anglaise travaillant en France a saisi le Conseil des Prud'hommes pour licenciement abusif.

Il est fréquent qu'une entreprise détienne plusieurs Le blog litigieux, « petiteanglaise.com », permettait à son auteur de partager son expérience d'expatriée et ne contenait que très peu d'éléments relatifs à sa vie professionnelle.

Par une décision du 30 mars 2007, le Conseil des Prud'hommes a considéré que le licenciement était abusif et a condamné l'employeur à 44.000 euros de dommages et intérêts.

Cette affaire rappelle que le principe de liberté d'expression s'applique à tous les écrits, même diffusés sur un blog.

Ce principe de liberté d'expression est énoncé par

l'article 11 de la Déclaration des droits de l'homme et reconnu par l'article 10 de la Convention européenne des droits de l'homme. Il trouve sa traduction dans la loi du 29 juillet 1881 relative à la liberté de la presse.

Cette loi a pour objectif de concilier la liberté d'expression avec le respect des droits fondamentaux de la personne (droit à l'image, respect de la vie privée, de l'honneur et de la réputation, présomption d'innocence...) et la protection de l'ordre public.

Ces dispositions ont été appliquées dans la décision du Conseil des Prud'hommes de Paris le 13 mai 2005, considérant comme abusif le licenciement prononcé à l'encontre de Daniel Schneidermann, chroniqueur du journal « Le Monde » suite à la publication d'un livre dans lequel il critiquait certaines positions prises par la direction du journal.

Par ailleurs, dans l'affaire « petiteanglaise.com », l'employeur estimait que le fait de rédiger certains des articles du blog sur le lieu et durant les heures de travail constituait des éléments supplémentaires apportant une cause réelle et sérieuse au licenciement.

Cet argument a été écarté, conformément à la décision du Conseil des Prud'hommes de Nanterre du 16 juillet 1999 selon laquelle le fait d'alimenter un blog ou de le consulter sur son lieu de travail ne justifie pas un licenciement pour faute du salarié, à moins qu'une clause du contrat de travail ou de règlement intérieur ne le prohibe expressément.

De manière générale, la tenue d'un blog par un salarié n'est donc pas en soi une cause réelle et sérieuse pouvant motiver un licenciement, sauf si les propos qu'il contient portent atteinte aux droits fondamentaux susvisés.

Enfin, on peut imaginer la validation du licenciement si le temps passé par le salarié à alimenter son blog sur son lieu de travail est excessif et nuit gravement à sa prestation de travail.



ADRESSAGE, NOMS DE DOMAINE ET LIENS HYPERTEXTES, PROPRIÉTÉS INDUSTRIELLES ET COMMERCIALES

PREMIER CAS DE SUCKS EN .EU

Par M. Benjamin Vitasse, Juriste
- Consultant noms de domaine

Après quelques 600 décisions relatives aux .eu, la première affaire en « suck » vient d'être rendue par la Cour d'Arbitrage Tchèque
(http://adreu.eurid.eu/adr/decisions/decision.php?dispute_id=4141)

La pratique consiste à enregistrer un nom (généralement une marque connue) et d'y ajouter « suck » ou « sucks » (terme d'argot anglais signifiant que quelque chose est mauvais), généralement dans le but de critiquer la société visée.

L'affaire porte sur deux noms de domaine, airfrancesucks.eu et airfrance-jp.eu, enregistrés (mais non exploités) par Lexicon Media Ltd.

Sans grande surprise Air France a obtenu le transfert des noms de domaine. Pour autant, cette affaire apporte un éclairage intéressant sur le cas spécifique des noms en « sucks » et plus généralement sur la rétention passive (« passive holding ») des noms de domaine.

L'expert désigné pour trancher ce litige, David-Irving Tayer, doit déterminer si le nom « airfrancesucks.eu » est de nature à induire l'internaute en erreur. Sur ce point, il estime que le simple fait d'ajouter un terme péjoratif au nom de la société n'est pas suffisant pour écarter le risque de confusion.

Dans le même sens, la récente décision UDRP du 09

avril 2007 « airfrancesuck.com » souligne que pour un internaute français le terme « suck » peut être interprété tout à fait différemment, au sens d'un acronyme par exemple (tel que GmbH, S.A, SARL ...). Le nom pourrait alors être perçu comme « Air Frances Uck » et donc entraîner un risque de confusion.

L'arbitre décide ensuite que le défendeur n'avait aucun droit ou intérêt légitime sur les noms et que ceux-ci avaient été enregistrés et utilisés de mauvaise foi.

Rappelons que les noms litigieux n'étaient pas exploités. Comment retenir donc l'utilisation de mauvaise foi... à défaut d'exploitation ?

Selon David-Irving Tayer, l'utilisation de mauvaise foi d'un nom de domaine se juge au regard d'éléments matériels, tels que la mise en place de pages parking, de pages statiques, de mention « en construction », ...

Pour autant, un nom de domaine enregistré mais non exploité n'est pas systématiquement considéré comme une exploitation de mauvaise foi. La jurisprudence *Locatour* s'était déjà prononcée en ce sens, en se basant sur le principe de spécialité du droit des marques.

Par ailleurs, un défaut d'exploitation peut tout à fait se justifier par un besoin de confidentialité ou tout simplement un délai nécessaire entre le moment où le nom est enregistré et la mise en ligne des pages web afférentes.

En l'espèce, rien ne prouve que les noms avaient été réservés pour critiquer l'action de la compagnie aérienne (ce qui est toléré au regard de la liberté d'expression).

David-Irving Tayer retient que les noms avaient été enregistrés dans le but de perturber l'activité d'Air France et ordonne leur rétrocession à cette dernière.

Décret n° 2007-663 du 2 mai 2007 Pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie, J.O n° 104 du 4 mai 2007 p. 7865

Le Premier ministre,

Vu le règlement (CE) n° 1334/2000 du Conseil du 22 juin 2000 modifié instituant un régime communautaire de contrôles des exportations de biens et technologies à double usage ;

Vu la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 modifiée prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la défense ;

Vu le code pénal, notamment ses articles L. 131-21, L. 226-13 et R. 610-1 ;

Vu la loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique, notamment ses articles 30, 31, 36 et 40 ;

Vu le décret n° 95-589 du 6 mai 1995 modifié relatif à l'application du décret-loi du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions ;

Vu le décret n° 96-67 du 29 janvier 1996 modifié relatif aux compétences du secrétaire général de la défense nationale dans le domaine de la sécurité des systèmes d'information ;

Vu le décret n° 2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Vu le décret n° 2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information ;

Vu le décret n° 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage ;

Vu la notification à la Commission européenne n° 2006/0253/F du 29 mai 2006 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

Chapitre Ier : Régime de dispense de toute formalité préalable

Article 1

Sont dispensées des formalités préalables prévues aux chapitres II et III du présent décret les opérations de fourniture, de transfert, d'importation ou d'exportation des moyens et prestations de cryptologie mentionnées à l'annexe 1 du présent décret.

Article 2

Sont dispensées des mêmes formalités les opérations de transfert, d'importation et d'exportation des moyens de cryptologie qui ont fait l'objet d'une autorisation d'importation ou d'exportation en application des dispositions des articles L. 2335-1 à L. 2335-3 du code de la défense.

Chapitre II : Régime de déclaration

Article 3

Sont soumises à déclaration préalable, dans les conditions fixées au présent chapitre :

1° Les opérations, non mentionnées au chapitre Ier du présent décret, de fourniture, de transfert depuis un Etat membre de la Communauté européenne et d'importation de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité ;

2° Les opérations de transfert ou d'exportation de moyens de cryptologie mentionnées à l'annexe 2 du présent décret ;

3° La fourniture de prestations de cryptologie non mentionnées à l'annexe 1 du présent décret.

Article 4

Un mois au moins avant l'opération mentionnée à l'article 3, le dossier de déclaration est adressé par envoi recommandé avec demande d'avis de réception ou déposé contre accusé de dépôt à la direction centrale de la sécurité des systèmes d'information au secrétariat général de la défense nationale. Cette direction en délivre récépissé revêtu du numéro d'enregistrement du dossier.

La forme et le contenu du dossier de déclaration sont définis par un arrêté du Premier ministre. Ce dossier comporte une partie technique et une partie administrative.

Article 5

Dans le délai d'un mois à compter de la réception du dossier de déclaration, si le dossier est incomplet, la direction centrale de la sécurité des systèmes d'information invite le déclarant, par lettre recommandée avec demande d'avis de réception, à fournir les pièces complémentaires. Dans ce cas, le délai d'un mois prévu au premier alinéa de l'article 4 court à compter de la réception des pièces complémentaires.

Si le moyen de cryptologie déclaré relève du régime de l'autorisation, la direction centrale de la sécurité des systèmes d'information, dans le délai d'un mois à compter de la date à laquelle le dossier a été reçu ou, le cas échéant, complété, invite le déclarant, par lettre recommandée avec demande d'avis de réception, à procéder à l'application des dispositions du chapitre III.

A l'expiration du délai d'un mois, en cas de silence de la direction centrale de la sécurité des systèmes d'information, le déclarant peut procéder librement aux opérations faisant l'objet de la déclaration. La direction

centrale de la sécurité des systèmes d'information peut, le cas échéant, avant l'expiration de ce délai, délivrer au déclarant une attestation confirmant que celui-ci s'est acquitté de son obligation déclarative.

Article 6

La déclaration de fourniture d'un moyen de cryptologie effectuée conformément aux dispositions du présent chapitre vaut, dans les mêmes conditions, déclaration pour les intermédiaires qui assurent, le cas échéant, la diffusion du moyen de cryptologie fourni par le déclarant.

Article 7

Pour les opérations mentionnées au 1° et au 2° de l'article 3, le Premier ministre peut demander au déclarant, par lettre recommandée avec demande d'avis de réception, dans un délai d'un an à compter de la date de réception du dossier complet de déclaration prévu à l'article 4 :

1° De lui communiquer, dans un délai de deux mois, les caractéristiques techniques et le code source du moyen de cryptologie qui a fait l'objet de la déclaration ;

2° De mettre à la disposition de la direction centrale de la sécurité des systèmes d'information deux exemplaires du moyen de cryptologie pour une durée qui ne peut excéder six mois.

Lorsque les éléments fournis par le déclarant sont incomplets, le Premier ministre dispose d'un délai de deux mois à compter de leur réception pour demander au déclarant, par lettre recommandée avec demande d'avis de réception, de lui communiquer des éléments complémentaires dans un délai de deux mois.

Un arrêté du Premier ministre précise la nature des caractéristiques techniques mentionnées au 1°, qui portent sur la description complète de la mise en oeuvre du moyen de cryptologie ainsi que sur ses fonctions ou procédés de cryptologie.

Article 8

Les délais d'un mois prévus aux articles 4 et 5 sont portés à deux mois lorsque la déclaration concerne la fourniture de prestations de cryptologie.

Ces délais sont également portés à deux mois lorsque la déclaration concerne l'exportation de moyens de cryptologie vers des Etats non membres de la Communauté européenne. Dans ce cas, le délai d'un an prévu au premier alinéa de l'article 7 est réduit à deux mois.

Chapitre III : Régime d'autorisation**Article 9**

Le dossier de demande d'autorisation est adressé par envoi recommandé avec demande d'avis de réception ou déposé contre accusé de dépôt à la direction centrale de la sécurité des systèmes d'information. Cette dernière en délivre récépissé revêtu du numéro d'enregistrement du dossier.

La forme et le contenu du dossier de demande d'autorisation sont définis par un arrêté du Premier ministre. Ce dossier comporte une partie technique et une partie administrative.

Article 10

Si le dossier est complet, le Premier ministre notifie sa décision, par lettre recommandée avec demande d'avis de réception, dans un délai de quatre mois à compter de la délivrance de l'avis de réception ou de l'accusé de dépôt de la demande. Un défaut de notification dans ce délai vaut autorisation pour une durée d'un an.

Le dossier est réputé complet si, dans le délai de deux mois suivant la réception de la demande, la direction centrale de la sécurité des systèmes d'information n'a pas invité, par lettre recommandée avec demande d'avis de réception, le demandeur à fournir des pièces complémentaires. Dans ce dernier cas, le délai de quatre

mois fixé à l'alinéa précédent court à compter de la réception des pièces complétant le dossier.

Le Premier ministre peut également requérir le demandeur, dans le délai de deux mois mentionné à l'alinéa précédent, de mettre à la disposition de la direction centrale de la sécurité des systèmes d'information le code source et, pour une durée qui ne peut excéder six mois, deux exemplaires du moyen de cryptologie.

Article 11

L'autorisation peut être assortie de conditions visant à assurer la protection des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat.

Elle est délivrée pour une durée qui ne peut excéder cinq années. Elle peut être renouvelée dans les mêmes conditions que la demande initiale.

Article 12

L'autorisation peut être retirée par le Premier ministre :

- 1° En cas de fausse déclaration ou de faux renseignement ;
- 2° Lorsque son maintien risque de porter atteinte à la défense nationale ou à la sécurité intérieure ou extérieure de l'Etat ;
- 3 En cas de non-respect des prescriptions dont est, le cas échéant, assortie l'autorisation ;
- 4° Lorsque le titulaire de l'autorisation cesse l'exercice de l'activité pour laquelle a été délivrée l'autorisation ;
- 5° Lorsque les conditions auxquelles est subordonnée la délivrance de l'autorisation ne sont plus réunies.

Le retrait ne peut intervenir qu'après que le titulaire de l'autorisation a été mis à même de faire valoir ses observations dans un délai de huit jours.

En cas d'urgence, l'autorisation peut être suspendue immédiatement.

Chapitre IV : Dispositions pénales

Article 13

Le fait de fournir des prestations de cryptologie ne visant pas à assurer des fonctions de confidentialité sans avoir satisfait à l'obligation de déclaration prévue aux articles 3 et 4 est puni des peines prévues pour les contraventions de la 5e classe.

Les personnes coupables de l'infraction prévue à l'alinéa précédent encourent également la peine complémentaire de confiscation, suivant les modalités prévues par l'article L. 131-21 du code pénal, de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.

Chapitre V : Dispositions diverses et transitoires

Article 14

L'habilitation prévue au premier alinéa de l'article 36 de la loi du 21 juin 2004 susvisée est accordée par arrêté du Premier ministre à des agents en fonction à la direction centrale de la sécurité des systèmes d'information.

Cette habilitation peut être retirée à tout moment par décision du Premier ministre.

Les agents habilités prêtent devant le tribunal de grande instance dans le ressort duquel se trouve leur résidence administrative le serment suivant : « Je jure et promets de bien et loyalement remplir mes fonctions et d'observer, en tout, les devoirs qu'elles m'imposent. Je jure également de ne rien révéler ou utiliser de ce qui sera porté à ma connaissance à l'occasion de l'exercice de mes fonctions. » La prestation de serment est enregistrée sans frais au greffe du tribunal, l'acte de ce serment est dispensé du timbre et d'enregistrement, il est transcrit gratuitement sur les commissions d'emploi visées à l'alinéa suivant.

Dans l'exercice de leurs fonctions, ces agents doivent être munis de leur commission d'emploi faisant mention de leur habilitation et de leur prestation de serment. Ils sont tenus de la présenter à la première réquisition.

Article 15

Les agents de l'Etat veillent à la protection des informations à caractère secret qui sont recueillies dans le cadre des procédures prévues par le présent décret et dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal.

Article 16

L'accomplissement des formalités prévues par le présent décret ne dispense pas les intéressés de souscrire, s'il y a lieu, les autres déclarations prévues par la réglementation ni de solliciter les autres autorisations requises par les textes en vigueur, notamment en application des dispositions de l'article L. 2332-1 du code de la défense et du décret du 13 décembre 2001 susvisé pris pour l'application du règlement (CE) n° 1334/2000 susvisé.

Article 17

Les dispositions du présent décret s'appliquent aux demandes d'autorisation déposées avant sa date d'entrée en vigueur et pour lesquelles aucune décision, tacite ou expresse, n'est intervenue avant cette date. Les délais prévus par le présent décret commencent, en ce cas, à courir à compter de sa date d'entrée en vigueur.

Les titulaires d'autorisations d'importation ou de fourniture de moyens ou de prestations de cryptologie en cours de validité à la date d'entrée en vigueur du présent décret sont réputés avoir satisfait à l'obligation de déclaration prévue au chapitre II du présent décret lorsque celle-ci est requise pour l'opération concernée.

Article 18

A l'article 2 du décret du 6 mai 1995 susvisé, le d du paragraphe 4 de la deuxième catégorie du A est remplacé par les dispositions suivantes :

« d) Moyens de cryptologie : matériels ou logiciels permettant la transformation à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers ou réalisant l'opération inverse lorsqu'ils sont spécialement conçus ou modifiés pour porter, utiliser ou mettre en oeuvre les armes, soutenir ou mettre en oeuvre les forces armées, ainsi que ceux spécialement conçus ou modifiés pour le compte du ministère de la défense en vue de protéger les secrets de la défense nationale. »

Article 19

Au I de l'article 9 du décret du 30 mars 2001 susvisé, les mots : « l'article 28 de la loi du 29 décembre 1990 susvisée » sont remplacés par les mots : « l'article 31 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ».

Article 20

Dans tous les textes réglementaires, notamment à l'article 3 du décret du 31 juillet 2001 susvisé, la référence au décret n° 98-101 du 24 février 1998 est remplacée par la référence au présent décret et la référence au décret n° 98-102 du 24 février 1998 est supprimée.

Article 21

Les dispositions du présent décret sont applicables en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna, à Mayotte et dans les Terres australes et antarctiques françaises.

Article 22

Les décrets n° 98-101 du 24 février 1998, n° 98-102 du 24 février 1998, n° 99-199 du 17 mars 1999 et n° 99-200 du 17 mars 1999 sont abrogés.

Toutefois, les déclarations souscrites avant la date d'entrée en vigueur du présent décret demeurent régies par les dispositions du décret n° 98-101 du 24 février 1998.

Article 23

Le garde des sceaux, ministre de la justice, et le ministre de l'outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 2 mai 2007.

Dominique de Villepin

Par le Premier ministre :

Le garde des sceaux, ministre de la justice, Pascal Clément

Le ministre de l'outre-mer, Hervé Mariton

Décret n° 2007-602 du 25 avril 2007 relatif aux conditions et aux modalités de vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise et modifiant le code du travail (deuxième partie : Décrets en Conseil d'État), J.O n° 99 du 27 avril 2007 p. 7492

Le Premier ministre,

Sur le rapport du ministre de l'emploi, de la cohésion sociale et du logement,

Vu le code du travail, notamment ses articles L. 423-13 et L. 433-9 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2004-575 du 21 juin 2004 relative à la confiance dans l'économie numérique, notamment son article 54 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 14 septembre 2006 ;

Le Conseil d'Etat (section sociale) entendu,

Décète :

Article 1

Il est inséré au chapitre III du titre II du livre IV du code du travail, après l'article R. 423-1-1, un article R. 423-1-2 ainsi rédigé :

« Art. R. 423-1-2. - I. - L'élection prévue à l'article L. 423-13 peut être réalisée par vote électronique sur le lieu de travail ou à distance.

« La possibilité de recourir à un vote électronique est ouverte par un accord d'entreprise ou par un accord de groupe comportant un cahier des charges respectant les prescriptions minimales énoncées au présent article.

« La mise en place du vote électronique n'interdit pas le vote à bulletin secret sous enveloppe si l'accord n'exclut pas cette modalité.

« II. - La conception et la mise en place du système de vote électronique peuvent être confiées à un prestataire choisi par le chef d'entreprise sur la base d'un cahier des charges contenant les prescriptions énoncées au présent article.

« Le système retenu assure la confidentialité des données transmises, notamment de celles des fichiers constitués pour établir les listes électorales des collèges prévus à l'article L. 423-2, ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes.

« Les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement et de déchiffrement et le contenu de l'urne ne doivent être accessibles qu'aux personnes chargées de la gestion et de la maintenance du système.

« Le système de vote électronique doit pouvoir être scellé à l'ouverture et à la clôture du scrutin.

« Les données relatives aux électeurs inscrits sur les listes électorales ainsi que celles relatives à leur vote sont traitées par des systèmes informatiques distincts, dédiés et isolés, respectivement dénommés "fichier des électeurs et "contenu de l'urne électronique.

« Le système de vote électronique, préalablement à sa mise en place ou à toute modification substantielle de sa conception, est soumis à une expertise indépendante,

destinée à vérifier le respect des prescriptions énoncées ci-dessus. Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

« Les prescriptions énoncées ci-dessus s'imposent également aux personnes chargées de la gestion et de la maintenance du système informatique.

« III. - L'employeur met en place une cellule d'assistance technique chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique, comprenant, le cas échéant, les représentants du prestataire.

« IV. - Les organisations syndicales de salariés incluses dans le périmètre de l'accord mentionné au I et qui sont représentatives au sens de l'article L. 132-2 sont tenues informées par l'employeur de l'accomplissement des formalités déclaratives préalables auprès de la Commission nationale de l'informatique et des libertés.

« Chaque salarié dispose d'une notice d'information détaillée sur le déroulement des opérations électorales.

« Les représentants du personnel, les délégués syndicaux et les membres du bureau de vote bénéficient d'une formation sur le système de vote électronique retenu.

« V. - Le protocole d'accord préélectoral prévu à l'article L. 423-3 mentionne la conclusion de l'accord d'entreprise ou de l'accord de groupe autorisant le recours au vote électronique et, le cas échéant, le nom du prestataire choisi pour le mettre en place.

« Il comporte en annexe la description détaillée du fonctionnement du système retenu et du déroulement des opérations électorales.

« VI. - Le vote électronique se déroule, pour chaque tour de scrutin, pendant une période délimitée.

« En présence des représentants des listes de candidats, la cellule d'assistance technique prévue au III :

« 1° Procède, avant que le vote ne soit ouvert, à un test du système de vote électronique et vérifie que l'urne électronique est vide, scellée et chiffrée par des clés délivrées à cet effet ;

« 2° Procède, avant que le vote ne soit ouvert, à un test spécifique du système de dépouillement, à l'issue duquel le système est scellé ;

« 3° Contrôle, à l'issue des opérations de vote et avant les opérations de dépouillement, le scellement de ce système.

« La liste d'émargement n'est accessible qu'aux membres du bureau de vote et à des fins de contrôle du déroulement du scrutin.

« Aucun résultat partiel n'est accessible pendant le déroulement du scrutin. Toutefois, le nombre de votants peut, si l'accord prévu au I le prévoit, être révélé au cours du scrutin.

« Lorsque l'accord prévu au I n'exclut pas le vote au scrutin secret sous enveloppe, l'ouverture du vote n'a lieu qu'après la clôture du vote électronique. Le président du bureau de vote dispose, avant cette ouverture, de la liste d'émargement des électeurs ayant voté par voie électronique.

« VII. - L'employeur ou, le cas échéant, le prestataire qu'il a retenu conserve sous scellés, jusqu'à l'expiration du délai de recours et, lorsqu'une action contentieuse a été engagée, jusqu'à la décision juridictionnelle devenue définitive, les fichiers supports comprenant la copie des programmes sources et des programmes exécutables,

les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde. La procédure de décompte des votes doit, si nécessaire, pouvoir être exécutée de nouveau.

« A l'expiration du délai de recours ou, lorsqu'une action contentieuse a été engagée, après l'intervention d'une décision juridictionnelle devenue définitive, l'employeur ou, le cas échéant, le prestataire procède à la destruction des fichiers supports.

« VIII. - Un arrêté du ministre chargé du travail, pris après avis de la Commission nationale de l'informatique et des libertés, précise les dispositions pratiques de mise en oeuvre du vote électronique. »

Article 2

Il est inséré au chapitre III du titre II du livre IV du même code, après l'article R. 433-2-1, un article R. 433-2-2 ainsi rédigé :

« Art. R. 433-2-2. - I. - L'élection prévue à l'article L. 433-9 peut être réalisée par vote électronique sur le lieu de travail ou à distance.

« La possibilité de recourir à un vote électronique est ouverte par un accord d'entreprise ou par un accord de groupe comportant un cahier des charges respectant les prescriptions minimales énoncées au présent article.

« La mise en place du vote électronique n'interdit pas le vote à bulletin secret sous enveloppe si l'accord n'exclut pas cette modalité.

« II. - La conception et la mise en place du système de vote électronique peuvent être confiées à un prestataire choisi par le chef d'entreprise sur la base d'un cahier des

charges contenant les prescriptions énoncées au présent article.

« Le système retenu assure la confidentialité des données transmises, notamment de celles des fichiers constitués pour établir les listes électorales des collèges prévus à l'article L. 433-2, ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes.

« Les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement et de déchiffrement et le contenu de l'urne ne doivent être accessibles qu'aux personnes chargées de la gestion et de la maintenance du système.

« Le système de vote électronique doit pouvoir être scellé à l'ouverture et à la clôture du scrutin.

« Les données relatives aux électeurs inscrits sur les listes électorales ainsi que celles relatives à leur vote sont traitées par des systèmes informatiques distincts, dédiés et isolés, respectivement dénommés "fichier des électeurs et "contenu de l'urne électronique.

« Le système de vote électronique, préalablement à sa mise en place ou à toute modification substantielle de sa conception, est soumis à une expertise indépendante, destinée à vérifier le respect des prescriptions énoncées ci-dessus. Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

« Les prescriptions énoncées ci-dessus s'imposent également aux personnes chargées de la gestion et de la maintenance du système informatique.

« III. - L'employeur met en place une cellule d'assistance technique chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique,

comprenant, le cas échéant, les représentants du prestataire.

« IV. - Les organisations syndicales de salariés incluses dans le périmètre de l'accord mentionné au I et qui sont représentatives au sens de l'article L. 132-2 sont tenues informées par l'employeur de l'accomplissement des formalités déclaratives préalables auprès de la Commission nationale de l'informatique et des libertés.

« Chaque salarié dispose d'une notice d'information détaillée sur le déroulement des opérations électorales.

« Les représentants du personnel et les membres du bureau de vote bénéficient d'une formation sur le système de vote électronique retenu.

« V. - Le protocole d'accord préélectoral prévu à l'article L. 433-2 mentionne la conclusion de l'accord d'entreprise ou de l'accord de groupe autorisant le recours au vote électronique et, le cas échéant, le nom du prestataire choisi pour le mettre en place.

« Il comporte en annexe la description détaillée du fonctionnement du système retenu et du déroulement des opérations électorales.

« VI. - Le vote électronique se déroule, pour chaque tour de scrutin, pendant une période délimitée.

« En présence des représentants des listes de candidats, la cellule d'assistance technique prévue au III :

« 1° Procède, avant que le vote ne soit ouvert, à un test du système de vote électronique et vérifie que l'urne électronique est vide, scellée et chiffrée par des clés délivrées à cet effet ;

« 2° Procède, avant que le vote ne soit ouvert, à un test spécifique du système de dépouillement à l'issue duquel le système est scellé ;

« 3° Contrôle, à l'issue des opérations de vote et avant les opérations de dépouillement, le scellement de ce système.

« La liste d'émargement n'est accessible qu'aux membres du bureau de vote et à des fins de contrôle de déroulement du scrutin.

« Aucun résultat partiel n'est accessible pendant le déroulement du scrutin. Toutefois, le nombre de votants peut, si l'accord prévu au I le prévoit, être révélé au cours du scrutin.

« Lorsque l'accord prévu au I n'exclut pas le vote au scrutin secret sous enveloppe, l'ouverture du vote n'a lieu qu'après la clôture du vote électronique. Le président du bureau de vote dispose, avant cette ouverture, de la liste d'émargement des électeurs ayant voté par voie électronique.

« VII. - L'employeur ou, le cas échéant, le prestataire qu'il a retenu conserve sous scellés, jusqu'à l'expiration du délai de recours et, lorsqu'une action contentieuse a été engagée, jusqu'à la décision juridictionnelle devenue définitive, les fichiers supports comprenant la copie des programmes sources et des programmes exécutables, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde. La procédure de décompte des votes doit, si nécessaire, pouvoir être exécutée de nouveau.

« A l'expiration du délai de recours ou, lorsqu'une action contentieuse a été engagée, après l'intervention d'une décision juridictionnelle devenue définitive, l'employeur ou, le cas échéant, le prestataire procède à la destruction des fichiers supports.

« VIII. - Un arrêté du ministre chargé du travail, pris après avis de la Commission nationale de l'informatique et des libertés, précise les dispositions pratiques de mise en oeuvre du vote électronique. »

Article 3

Le ministre de l'emploi, de la cohésion sociale et du logement est chargé de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 25 avril 2007

Dominique de Villepin

Par le Premier ministre :

Le ministre de l'emploi, de la cohésion sociale et du logement, Jean-Louis Borloo

Arrêté du 25 avril 2007 pris en application du décret n° 2007-602 du 25 avril 2007 relatif aux conditions et aux modalités de vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise et modifiant le code du travail (deuxième partie : Décrets en Conseil d'État), J.O n° 99 du 27 avril 2007 p. 7494

Le ministre de l'emploi, de la cohésion sociale et du logement,

Vu le code du travail, et notamment ses articles L. 423-13 et L. 433-9 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2004-575 du 21 juin 2004 relative à la confiance dans l'économie numérique, notamment son article 54 ;

Vu le décret n° 2007-602 du 25 avril 2007 relatif aux conditions et aux modalités de vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise et modifiant le code du travail (deuxième partie : Décrets en Conseil d'Etat) ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 14 septembre 2006,

Arrête :

Article 1

En application du décret du 25 avril 2007 susvisé, les élections des délégués du personnel et des représentants du personnel au comité d'entreprise

peuvent être organisées par voie électronique sur place ou à distance selon les dispositions techniques de mise en oeuvre et les garanties fixées par le présent arrêté.

Article 2

Le traitement « fichier des électeurs » est établi à partir des listes électorales. Il a pour finalité de délivrer à chaque électeur un moyen d'authentification, d'identifier les électeurs ayant pris part au vote et d'éditer les listes d'émargement. L'émargement indique la date et l'heure du vote. Les listes sont enregistrées sur un support distinct de celui de l'urne électronique, scellé, non réinscriptible, rendant son contenu inaltérable et probant.

Les données du vote font l'objet d'un chiffrement dès l'émission du vote sur le poste de l'électeur.

Le fichier dénommé « contenu de l'urne électronique » recense les votes exprimés par voie électronique. Les données de ce fichier font l'objet d'un chiffrement et ne doivent pas comporter de lien permettant l'identification des électeurs afin de garantir la confidentialité du vote.

Article 3

Les listes électorales sont établies par l'employeur. Le contrôle de la conformité des listes importées sur le système de vote électronique aux listes électorales transmises le cas échéant au prestataire est effectué sous la responsabilité de l'employeur. L'intégration et le contrôle des candidatures sont effectués dans les mêmes conditions.

La mise en oeuvre du système de vote électronique est opérée sous le contrôle effectif, tant au niveau des moyens informatiques centraux que de ceux

éventuellement déployés sur place, de représentants de l'organisme mettant en place le vote. Toutes les mesures sont prises pour leur permettre de vérifier l'effectivité des dispositifs de sécurité prévus.

Tout système de vote électronique comporte un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et les mêmes caractéristiques.

En cas de dysfonctionnement informatique résultant d'une attaque du système par un tiers, d'une infection virale, d'une défaillance technique ou d'une altération des données, le bureau de vote a compétence, après avis des représentants susmentionnés, pour prendre toute mesure d'information et de sauvegarde et notamment pour décider la suspension des opérations de vote.

Article 4

Les données devant être enregistrées sont les suivantes :

- pour les listes électorales : noms et prénoms des inscrits, date d'entrée dans l'entreprise, date de naissance, collègue ;

- pour le fichier des électeurs : noms, prénoms, collègue, moyen d'authentification et, le cas échéant, coordonnées ;

- pour les listes d'émargement : collègue, noms et prénoms des électeurs ;

- pour les listes des candidats : collègue, noms, prénoms des candidats, titulaires ou suppléants, appartenance syndicale le cas échéant ;

- pour les listes des résultats : noms et prénoms des candidats, élus, non élus, voix obtenues, appartenance syndicale le cas échéant, collègue, destinataires mentionnés à l'article 5.

Article 5

Les destinataires ou catégories de destinataires de ces informations sont les suivants :

- pour les listes électorales : électeurs, syndicats représentatifs le cas échéant, agents habilités des services du personnel ;

- pour le fichier des électeurs : électeurs pour les informations les concernant ;

- pour les listes d'émargement : membres des bureaux de vote, agents habilités des services du personnel ;

- pour les listes des candidats : électeurs, syndicats, agents habilités des services du personnel ;

- pour les listes des résultats : électeurs, services du ministère chargé de l'emploi, syndicats, employeurs ou agents habilités des services du personnel.

En cas de contestation des élections, ces pièces sont tenues à la disposition du juge.

Article 6

Les heures d'ouverture et de fermeture du scrutin électronique doivent pouvoir être contrôlées par les membres du bureau de vote et les personnes désignées ou habilitées pour assurer le contrôle des opérations électorales.

Pour se connecter sur place ou à distance au système de vote, l'électeur doit se faire connaître par le moyen d'authentification qui lui aura été transmis, selon des modalités garantissant sa confidentialité. Ce moyen d'authentification permettra au serveur de vérifier son identité et garantira l'unicité de son vote. Il est alors impossible à quiconque de voter de nouveau avec les mêmes moyens d'authentification.

L'électeur accède aux listes de candidats et exprime son vote. Son choix doit apparaître clairement à l'écran ; il peut être modifié avant validation. La transmission du vote et l'émargement font l'objet d'un accusé de réception que l'électeur a la possibilité de conserver.

Tout électeur atteint d'une infirmité le mettant dans l'impossibilité de voter peut se faire assister par un électeur de son choix.

Le vote est anonyme et chiffré par le système, avant transmission au fichier « contenu de l'urne électronique » dans les conditions fixées à l'article 2, alinéa 3. La validation le rend définitif et empêche toute modification.

Article 7

Dès la clôture du scrutin, le contenu de l'urne, les listes d'émargement et les états courants gérés par les serveurs sont figés, horodatés et scellés automatiquement sur l'ensemble des serveurs.

Le dépouillement n'est possible que par l'activation conjointe d'au moins deux clés de chiffrement différentes sur les trois qui doivent être éditées.

La génération des clés destinées à permettre le dépouillement des votes à l'issue du scrutin est publique de manière à prouver de façon irréfutable que seuls le président du bureau de vote et deux de ses assesseurs

ont connaissance de ces clés à l'exclusion de toute autre personne, y compris du personnel technique chargé du déploiement du système de vote.

Ces deux assesseurs nominativement identifiés, le plus âgé et le plus jeune parmi les assesseurs à défaut d'accord, ainsi que le président du bureau de vote reçoivent chacun une clé de dépouillement distincte, selon des modalités en garantissant la confidentialité, permettant d'accéder aux données du fichier dénommé « contenu de l'urne électronique ». La présence de deux titulaires de ces clés est indispensable pour autoriser le dépouillement. Des clés de sauvegarde sont en outre conservées sous scellés.

Le décompte des voix apparaît lisiblement à l'écran et fait l'objet d'une édition sécurisée afin d'être porté au procès-verbal.

Le système de vote électronique est scellé après le dépouillement afin de garantir l'impossibilité de reprendre ou de modifier les résultats après la décision de clôture du dépouillement. La procédure de décompte des votes enregistrés doit pouvoir être déroulée de nouveau.

Article 8

Le directeur général du travail est chargé de l'exécution du présent arrêté, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 25 avril 2007.

Jean-Louis Borloo

DÉLIBÉRATION CNIL

Dél. n°2007-091 du 25 avril 2007 refusant la mise en oeuvre par l'Autorité de contrôle des assurances et des mutuelles (ACAM) d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au réseau informatique (postes de travail fixes et portables). ayant pour finalité la mise en place d'un dispositif d'alerte professionnelle

Thèmes

Informatique et libertés, Droits de la personnalité

Abstract

Biométrie, empreinte digitale, contrôle de l'accès au réseau informatique, refus d'autorisation

Résumé

L'Autorité de contrôle des assurances et des mutuelles (ACAM) ne peut mettre en oeuvre un traitement reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au réseau informatique

Délibération 2007-091 du 25 avril 2007

Délibération refusant la mise en oeuvre par l'Autorité de contrôle des assurances et des mutuelles (ACAM) d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au réseau informatique (postes de travail fixes et portables).

La Commission nationale de l'informatique et des libertés,

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment son article 25-8° ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 modifiée par le décret n° 2007-451 du 25 mars 2007 ;

Vu la demande d'autorisation, présentée par l'Autorité de contrôle des assurances et des mutuelles (ACAM) d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au réseau informatique (postes de travail fixes et portables) ;

Après avoir entendu M. Hubert BOUCHET, commissaire en son rapport et Mme Pascale COMPAGNIE, commissaire du Gouvernement, en ses observations.

Formule les observations suivantes :

La Commission nationale de l'informatique et des libertés a été saisie par l'Autorité de contrôle des assurances et des mutuelles (ACAM) d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès au réseau informatique (postes de travail fixes et portables).

Il y a lieu de faire application des dispositions prévues à l'article 25-8° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

L'ACAM est chargée de contrôler le respect par les entreprises d'assurance et de réassurance, les mutuelles, les institutions de prévoyance et les institutions de prévoyance et les institutions de retraite supplémentaire, des dispositions législatives et réglementaires qui leur sont applicables et de sanctionner les manquements constatés.

Le dispositif a pour objet de contrôler l'accès au réseau informatique (postes de travail fixes et portables).

La Commission considère que la constitution de bases de données d'empreintes digitales ne peut être admise que dans certaines circonstances particulières où l'exigence d'identification des personnes résulte d'un fort impératif de sécurité, conformément aux dispositions de l'article 6-3° de la loi du 6 janvier 1978 modifiée. En effet, cet article dispose que les traitements ne peuvent porter que sur des données à caractère personnel adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs.

En l'espèce, l'objectif poursuivi par l'ACAM tendant au contrôle de l'accès au réseau informatique (postes de travail fixes et portables), s'il est légitime, n'est associé à aucune circonstance particulière justifiant la conservation dans une base de données des empreintes digitales des

employés habilités à accéder au réseau informatique (postes de travail fixes et portables). En conséquence, le traitement pris dans son ensemble n'apparaît ni adapté ni proportionné à l'objectif poursuivi.

Dès lors, la Commission n'autorise pas, en l'état, l'Autorité de contrôle des assurances et des mutuelles (ACAM) sise au 54 rue de Châteaudun 75436 Paris Cedex 09, à mettre en oeuvre un traitement de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance des empreintes digitales et dont la finalité est le contrôle de l'accès au réseau informatique (postes de travail fixes et portables).
Le Président, Alex TURK.

Délibération également disponible sur Légifrance - <http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCP07040091A>

Référence : CNIL, 25 avril 2007, *REFUSANT LA MISE EN OEUVRE PAR ACAM D'UN TRAITEMENT AUTOMATISÉ DE DONNÉES À CARACTÈRE PERSONNEL REPOSANT SUR LA RECONNAISSANCE DES EMPREINTES DIGITALES ET AYANT POUR FINALITÉ LE CONTRÔLE DE L'ACCÈS*, DROIT-TIC

http://www.droit-tic.com/juris/aff.php?id_juris=100